The Community Cyber Security Maturity Model

Conference Paper · January 2007

DOI: 10.1109/HICSS.2007.522 · Source: DBLP

1 author:

Gregory White
University of Texas at San Antonio
38 PUBLICATIONS **246** CITATIONS

The Community Cyber Security Maturity Model

Gregory B. White, Ph.D.
The Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
greg.white@utsa.edu

Abstract

There have been an increasing number of articles in the press related to various threats and attacks on computer systems and networks. The critical infrastructures upon which our communities, states, and nation rely are increasingly dependent on computer systems and networks and are thus also increasingly vulnerable to cyber attacks upon them. Communities understand their responsibility in terms of being prepared to prevent, detect, and respond to most natural and man-made disasters but few understand what is involved in defending against cyber attacks. The Community Cyber Security Maturity Model provides a structure which communities and states can use to determine their level of preparedness and to create a plan to improve their security posture and enhance their chances of successfully preventing or detecting and responding to a cyber attack.

1. Introduction

Studies have shown that the highest rate of computer attacks have been directed against critical infrastructures such as government, financial services, manufacturing, and power.[1,2] In addition, the same studies have shown that the United States is the most targeted nation of such attacks. With the growing fear of terrorist attacks, the possibility of a cyber terrorist attack has been raised – especially in light of reports that extremists have called for the creation of hacker "armies" to plan cyberattacks against the U.S. government and have posted detailed instructions on how to conduct attacks on computer bulletin boards.[3] Lieutenant General Keith Alexander, the Director of the National Security Agency, stated that there are three areas in which he is particularly concerned with: terrorist attacks, a cyber attack, and a combined attack using cyber and other means.[4] All of this provides support for the challenges by various entities to have states and communities increase their efforts to develop effective cyber security programs. Unfortunately it is easy to issue a challenge to entities to secure their computer systems and networks and an entirely different matter to secure them.

Compounding the problem is a lack of standards against which a community can measure their current security status. There are a number of different best practice documents that organizations can refer to in order to evaluate individual organizations but there is no clear guidance for communities and states in this arena. This paper proposes a Community Cyber Security Maturity Model which communities can use to evaluate their current status and which can be used to build a program to improve their security posture. This model has been established based upon extensive experience working with states and communities developing and conducting cyber security exercises. The model proposes threats to be addressed, metrics, technology, training, and evaluation mechanisms for each of the five levels identified in the model.

2. Current Community Cyber Security Status

Local and state governments have a tremendous challenge in ensuring the protection of the critical computer systems and networks needed daily by their citizens. Almost always initial efforts are aimed at the systems owned or managed by government but the job is not complete at that point. The security of the public infrastructures, necessary to operate government computers and networks as well as the other critical infrastructures needed by the community, is also essential for government. These infrastructures include such things as power and water monitoring, control, and distribution systems. Community efforts to secure these and other critical infrastructures is complicated by the fact that often they are not owned by the community. In addition, the systems and networks of government agencies can be affected by many other systems within and outside of the community for which

1530-1605/07 $20.00 © 2007 IEEE

the local government has no control. Communication about threats and attacks on local government and critical infrastructure systems is difficult because of several factors. First, there is no sharing mindset. Organizations seldom want to make others aware of failures in their security. They generally see no advantage in doing this and there is not as much value to the organization that has had the problem as there is to others. Attacks often are not single events. What one organization is experiencing is likely also being experienced by others. If one entity discovers the attack communicating this information to others will help them determine whether it is also occurring to them. The second factor that makes sharing difficult is the fact that there is generally no effective way to share information between entities within a community. The Information Sharing and Analysis Centers (ISACs) that exist for several of the sectors do an effective job of sharing information within a given sector but are not designed to share between entities in a geographically defined community. Other organizations such as InfraGard, a community information sharing program sponsored by the FBI, has chapters in numerous communities but does not have an effective real-time sharing mechanism. All of these factors, the lack of understanding of the problem, a lack of technology and processes to share information and to detect attacks, and an isolationist mindset is the norm in communities and is what needs to be addressed before a cyber attack occurs.

3. Why a Maturity Model?

Maturity models are useful in guiding an organization in the development of processes leading to a state of maturity in the area for which the model was developed. Two good examples of maturity models are the Capability Maturity Model for Software (CMM or SW-CMM) [5] and the Systems Security Engineering Capability Maturity Model (SSE-CMM). [6] The Capability Maturity Model for Software was designed to provide "software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence." [5] This illustrates the goal for the model. It was needed because of the perceived lack of productivity and quality in the software development industry. The environment, known all to well by many in the software industry, was described as "reactionary, and managers are usually focused on solving immediate crises (better known as fire fighting). Schedules and budgets are routinely exceeded because they are not based on realistic estimates. When hard deadlines are imposed, product functionality and quality are often compromised to meet the schedule." [5] The model helps organizations develop a strategy to move from this immature software development state to a mature development state characterized by the productive development of quality software.

In addition to providing a roadmap for organizations to follow in developing mature processes, a maturity model also provides a basis from which to evaluate an organization's current status. The SSE-CMM, for example, was intended to be used for a number of things including as a "tool for engineering organizations to evaluate their security engineering practices" and as a "standard mechanism for customers to evaluate a provider's security engineering capability." In other words, for organizations to evaluate their current standing (maturity) in the area the model was designed to assist in.

Communities need similar help in developing security programs and processes that will enable them to effectively prevent, detect, respond to, and recover from cyber security events. They need to not only know where they currently stand in terms of their preparation but they need a roadmap to be able to follow to help them improve on their current status. It is for this purpose that the Community Cyber Security Maturity Model was developed.

4. The Community Cyber Security Maturity Model

As a result of the need to better define methods to determine the current status of a community in its cyber preparedness, and in order to provide a roadmap for communities to follow in their preparation efforts, the Community Cyber Security Maturity Model (CCSMM) was established. In order to address the many issues that a community faces, the model includes a number of different elements. The model needs to define not only the metrics that are used for measurement but the technology that is required, the threats that are being addressed, mechanisms to communicate between the disparate community entities, and tests that can be used along with the metrics to measure the current status of a community's security preparedness level. A more detailed discussion of each element of the model follows. It should be noted that a community can actually have organizations within the community that are at different levels in the model at the same time. Thus, the local government could be at one level while the industries or citizens in the community are at a completely different level. The model has the ability to

differentiate between the different community entities and their own level of preparedness.

4.1. The Five Maturity Levels

Each of the maturity levels in the model have been assigned a name indicative of the types of threats and activities being addressed at the level. The first level is labeled "Security Aware" which correctly implies that the major theme of activities at this level is to make individuals and organizations aware of the threats, problems, and issues related to cyber security. The second level is labeled "Process Development" and, again, provides a significant clue as to what the theme of this level is. Level 2 elements are designed to help communities establish and improve upon the security processes required to effectively address cyber security issues. Level 3 of the model is "Information Enabled" and indicates that organizations within the community are all aware of the issues related to security and have the processes and mechanisms in place to identify security relevant events. The goal at this level is to improve upon the information sharing mechanisms within the community to enable the community to effectively correlate seemingly disparate pieces of information. By doing so, a picture can be provided that might indicate an impending attack. Level 4 of the model is "Tactics Development". At this level elements are designed to develop better and more proactive methods to detect and respond to attacks. By this level most prevention methods should be in place. The top level of the model is "Full Security Operational Capability" and represents those elements that should be in place for any organization to consider itself fully operationally read y to address any type of cyber threat. This does not imply that entities at this level will be free from any successful attack but rather that they have done everything they could in order to prevent and detect attacks. In addition, communities at this level are in excellent shape to effectively respond in the event that they were not able to prevent an attack from succeeding in the first place. Organizations at this level will also be fully "plugged into" appropriate entities outside of the community so that information can be shared about attacks. This will allow all communities, by cooperatively working together, to address cyber security threats.

4.2. The Threats Addressed

The model is not as concerned with identifying specific threats that exist for computer systems and networks but rather with characterizing the various attacks that can occur. This characterization includes three elements: the type of individual who may be conducting the attack, the motivation of the individual, the amount of time that may be spent in setting up the attack, and the resources (money and equipment) that are necessary to conduct the attack. There are three categories of attacks identified in the model.

4.2.1. Unstructured Threats. The majority of attacks that organizations face are as a result of unstructured threats. Individuals that fall in this category include the unskilled "script kiddies", semi-skilled individuals who may be loosely affiliated with others, and disgruntled employees. Individuals in this category are characterized by having limited funds and time to conduct attacks, short term goals, and generally do not target the operation of an organization. The majority of time spent by organizations in security is addressed to this threat as it is the one that is most visible. Unfortunately it is often the only threat that organizations focus on and once these threats are adequately addressed, organizations will frequently assume that nothing else needs to be accomplished in terms of their security posture. This is far from the truth.

4.2.2. Structured Threats. The change from unstructured to structured threats is often not that extensive. It does not take much to go from a group of loosely affiliated individuals to an organized group with a specific goal or target. Threats in this category are characterized by planned, methodical attacks using systematic approaches to compromise, corrupt, or disrupt information or systems to gain information advantage and affect corporate operations. Individuals in this category are organized, often have funding to conduct their activities, and have a focused, long-term objective. Individuals that fall in this category include criminals, organized crime, activists ("hacktivists"), and in some cases competitors. For this category, the possibility of subverting or implanting an "insider" may occur. Some entities, such as the financial services and government sectors, have made attempts to address threats at this level in their security plans. Most organizations, however, have no plans for these threats.

4.2.3. Highly Structured Threats. The most serious threats include efforts that consist of planned, methodical, multi-disciplinary attacks designed to compromise, corrupt, disrupt, or destroy information or systems as part of a coordinated effort to gain information advantage and effect the operation of a sector. Attackers at this level are highly organized,

heavily funded, have extensive and often multi-disciplinary and multi-organization support, and generally have long-term, national security objectives motivating their attack. The attackers include terrorists and state-supported individuals. The attacks are also broader in this category and include coordinated physical, psychological, and cyber attacks. Cyber attacks at this level are much more difficult to mitigate as they will include large-scale Distributed Denial of Service (DDOS) and clandestine kernel-level system attacks. Few outside of the federal government consider the possibility of the types of attacks described for this category. In order to address highly-structured attacks, direct, organization and sector-wide responses – coordinated with both law enforcement and the national security and intelligence community – are required.

4.3. Metrics

The immediate question most ask is "at which level are we currently?" It is natural for communities to ask this question when presented with the model and it is important for them to know the answer. The answer to this question will help define the actions the community needs to take. To determine the appropriate level requires an evaluation of the current security posture of various entities within the community against a specified set of metrics. For many, the first step will actually be to begin measuring the various factors as outlined by the metrics indicated for the level in question. While some may already be measuring various factors, most communities currently do not have an active security measurement program in place. While the specifics vary, measurements include factors and activities that commonly occur on a daily basis but which might be affected should a cyber attack occur. This includes items such as the number of failed and successful login attempts, the number of "pings" a system received, and the number of port scans that occurred daily. Metrics will also include factors that fall under the category of network management but which are also useful for security. Examples of these metrics include average network usage (throughput), the number of emails sent and received, and the level of various types of network traffic (e.g. the number and type of ICMP packets). Metrics also include non-technical factors such as the number of employees that have received security training and the presence of certain professional organizations within the community (e.g. the existence of an Information Systems Security Association or InfraGard chapter).

4.4. Information Sharing

A basic premise of the CCSMM is that in order to effectively address cyber security attacks on a community, organizations within the community will have to share a certain type and amount of information. At this point, most communities have no idea what to share or how to share it. Some organizations within a community may be involved in organized information sharing efforts that exist within certain sectors. Many may be members of the various Information Sharing Analysis Centers (ISACs) that were created for the various critical infrastructures. The ISACs, however, are national entities and while there is some sharing of information between them at the national level, they are not set up to identify possible attacks on a community. As a result, an important part of the CCSMM is the development of various information sharing activities within the community. It begins at the lower level with simply the establishment of working groups to have individuals come together to discuss recent events that affect the community. It progresses through simple web-based or email-based information sharing mechanisms to more robust alerting systems at the higher levels.

4.5. Technology

The CCSMM recognizes that in order to develop and operate an effective program to address cyber threats, a certain amount of technology will be required. This includes not only the technology that is needed in order to protect individual systems and networks (which includes devices such as firewalls and intrusion detection systems) but the technology and mechanisms needed to implement an effective information sharing program. An important aspect of the program is to recognize that technology should not be simply point products deployed to address a specific threat and vulnerability with no relationship to other threats and vulnerabilities but should be integrated into an overall program so that each piece fits into a larger picture working toward a common goal.

4.6. Training

Training is an essential component of the CCSMM. Many administrators have only the barest of security training. Certainly there is no general understanding of the different categories of threats and what is required to address them. At each level of the CCSMM various training programs are identified. Some training is aimed at system and network administrators, other

training is targeted for first responders, government and industry leaders, or even the citizens within the community. Some training can be web-based and can have broad exposure within the community. Other training will be more focused and aimed at specific groups such as the first responders or network administrators. At level 1 of the model much of the training is designed to provide an initial awareness to members of the community about what the dangers of a cyber attack are. At the higher levels the training becomes much more technical and "hands-on".

4.7. Testing

Once a community has begun to implement metrics and training programs it will need to consider establishing a program to exercise and test its capabilities. At each level of the CCSMM an exercise is defined which will allow community leaders to evaluate their progress. At the lower levels of the model the tests consist of tabletop exercises. At the higher levels of the model the tests progress toward functional exercises incorporating more of the community at each level. Small drills and functional exercises should be conducted throughout the model at all levels for each organization within the community. For example, companies and organizations should on a regular basis test their backup plans ensuring that backups are useable and adequate to recover from a disaster of any type.

5. Using the CCSMM

A community consists of many different entities, not all of which may be at the same level of the model. A city's IT infrastructure, for example, might very well be at level 2 while local industry is still working toward implementation of the processes, training, and technology at level 1. Local government officials should encourage all entities within the community to strive to improve their security posture.

Just as organizations within a community will vary in their probability of being targeted for a cyber attack, communities are different with some being more likely to be a target of an attack than others. As a result, not all communities will need to maintain their preparedness efforts at a Level 5 *Full Security Operational Capability* status. In order to determine which level a community should be at, and the various organizations within the community, local officials who understand the current threat picture and who also understand the importance of various resources and entities within a community should conduct a threat assessment for the community itself. This threat assessment, which should be accomplished with input from state and federal law enforcement agencies, will help the community define what is most important, what are the most likely targets, and what needs to be protected (and to what level). With these objectives in mind, plans can be developed to bring each aspect of the community to their required level. Understanding the levels each needs to be at also helps define the goals for various tests and exercises that can be used to measure the effectiveness of established programs.

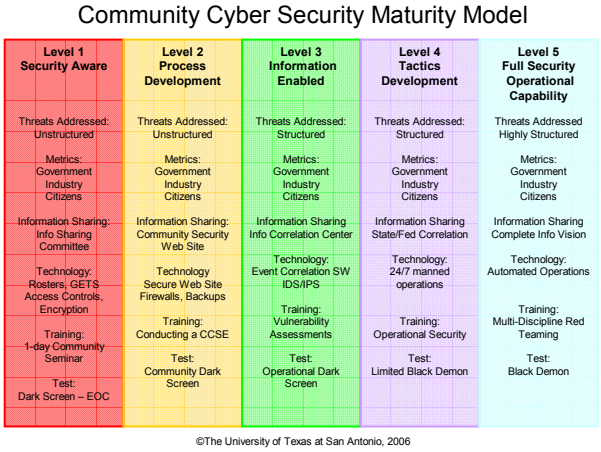

Figure 1. The Community Cyber Security Maturity Model

6. A Sample CCSMM Level

To better understand the components that make up each level of the CCSMM, it is useful to examine one of the levels in more detail. This is a working model under development and what will be required for an organization to reach a Level 5 state of preparedness is not yet fully defined. Certain aspects are understood but the training programs and technology needed for a community to be at this level have not yet been developed. Examination of a lower level, one in which there is already a fair understanding of the requirements is more realistic. For this paper, the first level, the one that communities will be striving for first, will be examined.

6.1. The Threat Addressed

The goal of Level 1 of the CCSMM is to have the community understand the security issues related to cyber security and to lay the foundations for a more robust security program. While a community may experience structured and highly structured threats, the main goal at this level is for communities to understand

the different threat levels but to concentrate on those measures that will allow them to deal with unstructured threats. This does not mean that they are not preparing to address the other levels of threats, the mechanisms they establish for unstructured threats will also be needed for the more intense threats as well. The purpose of stating that the threat to be addressed at this level is the unstructured threat is really to give the community a more realistic goal to obtain. Having them attempt to effectively deal with a highly structured threat is not realistic if most in the community don't understand the basics of computer threats. As long as people understand that there is more to accomplish and there are more organized threats that need to be eventually addressed, the goal has been accomplished at this level.

6.2. Metrics

In order to evaluate where the community is in relationship to their level of preparedness officials need to know what to measure and this requires that a set of metrics be established. Keeping the three broad categories of community entities allows for a more focused metrics program. For example, the local government needs to have a much more robust program and understanding of cyber threats than does the average citizen within the community. Since this level is focused on awareness and on the establishment of programs and processes that will be useful in later levels, the type of things that can be measured include whether the local government sponsors or has established an information sharing committee. This committee is important because it will be a constant battle to try and have people share information with others. Until this becomes second nature, people will need to be constantly reminded of the importance of information sharing, what needs to be shared, and the mechanisms that are in place to share that information. This information sharing committee can be informal in the sense that it be an advisory group consisting of individuals from the government (both local as well as any state or federal representatives that might be in the area), academia, and industry. It will not have any power to enforce any recommendations but will instead be used to advise the mayor/city manager on information sharing issues. Local officials should also appoint a cyber security point of contact within the local government (most likely a manager in the IT office, preferably the equivalent of a Chief Information Security Officer or CISO). Local law enforcement entities should also appoint a cyber crime point of contact. Both the law enforcement and local government cyber security points of contact should spend time in the community, with the support of the information sharing committee, to establish an awareness campaign addressing the importance of cyber security within the community. With the rise in cyber crime in the last few years, especially in the area of identity theft, programs such as this will be of interest to a large segment of the population and can serve as an introduction of the more general problem. A cyber crime (or cyber safety) web page should be established for the community or at the very least links to pages within federal and state agencies that deal with these issues.

Metrics for industry do not include community officials conducting assessments of local business networks. Officials do not have the time, nor the responsibility to secure the networks of every business within the community. Level 1 is an awareness level with the goal of ensuring that all understand that there is a cyber security problem that needs to be addressed. Consequently the measure of whether local industry understands the importance of cyber security as a topic and the need for information sharing can be something as simple as whether businesses participate in information sharing initiatives. One example of such an initiative is the information sharing committee the local government should be sponsoring. Another good measure is whether organizations such as local InfraGard chapters have been established. InfraGard addresses more than just cyber security issues so is important in many aspects of a community's security. One of their major goals, however, is information sharing and the establishment of an active InfraGard chapter is a good indication that at least those that participate understand the importance of the program.

The average citizen has very little responsibility at Level 1 of the model. Just as with local industry, the goal is merely awareness. Taking a poll, sending out random questionnaires, or conducting a survey are methods to measure the level of understanding of citizens but are not essential. Instead, if the community has an active program as exhibited by the other community sectors then an assumption can be made that some percentage of the community is being reached and through continued efforts the percentage should grow. Programs such as the web page previously mentioned, an outreach program by local law enforcement or city officials, and items such as public service announcements and commercials on local television and radio stations can serve to reach out to the members of the community. A sector that can be particularly useful in reaching out to citizens is academia which can sponsor seminars and classes on

cyber crime, online safety, identity theft, and higher level concepts such as critical infrastructure protection.

6.3. Information Sharing

Several information sharing mechanisms were addressed in the discussion of metrics. At this introductory level, however, it is important to again emphasize the need to constantly enforce the concept of information sharing and to understand that this will be an uphill battle. Sharing information is not a process that most are ingrained with. The normal response to most issues is to keep it as quiet as possible so others don't find out about it. While legislation is changing this somewhat – requiring in some instances that certain information be shared with civil penalties attached to the laws – it is still not a widely understood concept. Establishment of an InfraGard chapter and a community information sharing committee are first steps and any community programs they can conduct on the topic will help inculcate this into the community as a whole.

6.4. Technology

An important aspect of the CCSMM, especially at the higher levels, is that of the technology needed. Much of what is truly required to protect a community at Level 5 state has not been developed, or at least has not been organized into a useable product. At Level 1, however, what is needed is much more basic, since the concentration is on security awareness and an understanding of the importance of information sharing. As an example, a simple place to start is in developing a phone roster of cyber security points of contact within the community. Different rosters can be established for different purposes (for example, the average citizen really only needs to know who to call within the local government or law enforcement agency and does not need to know the security officer for all businesses within the community). Another simple part of the technology piece at Level 1 is the public web page that has already been discussed. Something that should be considered, especially by the individual organizations, is what is needed from a technical standpoint in order to maintain critical operations. Business Continuity Plans should be established by organizations and backup and recovery processes and procedures established. From an emergency responder perspective, communications are of extreme importance and mechanisms to ensure the ability to communicate in the event of a crisis should be reviewed to ensure that backup procedures are in place. A simple metric to see how well this is understood is whether local officials have obtained the Government Emergency Telecommunication Service (GETS) cards available to those with emergency preparedness missions. [7] While this service is not a panacea for communication problems, it does help in certain emergency situations and serves as a good indicator of whether a community has thought about these issues.

6.5. Training

There are many training programs both commercially available and through government agencies that can help communities understand the issue of cyber security. There are numerous security conferences, seminars, and web pages that are also useful. All of these can serve to help prepare a community and the various organizations within the community but at some point the issue of information sharing needs to be addressed and the responsibilities of the various organizations within the community explained. The Department of Homeland Security is currently having a variety of cyber security courses developed which are aimed at community and state entities. As these are completed they can be adopted as part of this model. Until they are, evidence of security training obtained from the various commercial sources can serve to establish the current community training level. An important aspect of training is not just the training of IT personnel but all users of computer systems and networks.

6.6. Test/Exercise

As those in the first responder community know, it is important for individuals to periodically practice response processes and procedures in order to be prepared to effectively respond when a real event occurs. It is also equally important to periodically test both personnel and the processes, procedures, and technology to ensure that they are adequate and able to respond to the situation and response being tested. In order to accomplish this, communities should incorporate cyber security exercises in their established exercise program. [8, 9] Exercises at Level 1 should be focused initially on awareness issues and after processes and procedures are established can be expanded to cover examination of their effectiveness and the level of preparedness of the appropriate response personnel.

6.7. Level 1 in Summary

As was discussed, Level 1 is the initial awareness level that all communities should be striving for. At this level much of what was discussed is of a non-technical level and focuses more on information sharing and communication rather than on the technical aspects of cyber security. Later levels will introduce the various mechanisms needed to effectively prevent attacks or to detect them and respond to them should prevention mechanisms fail. This introduction to Level 1 should serve to illustrate the type of issues addressed at each level and how they are intertwined throughout a community.

7. CCSMM Relationship to State Exercises

The model as illustrated in Figure 1 is designed for communities. It, however, can be used to implement a state cyber security program. States consist of individual communities, each of which should be working toward improving their own security posture. States can assist communities by doing such things as sponsoring training for communities, and conducting state exercises focusing on any of the levels of the model. Assistance for the communities will help provide consistency across the state and the leadership will be appreciated by communities, especially the smaller ones. State exercises can be conducted at any level which would consist of multiple community exercises being concurrently conducted along with a state cell for coordinating the activities of state agencies and the efforts of the communities.

8. Conclusion

Cyber attacks upon communities and the entities within them is a forgone conclusion. Whether the community will be ready for such an attack depends on what they do now to prepare. Most communities do not know where to start to prepare for such an event. The Community Cyber Security Maturity Model provides a framework which communities can use to evaluate their current level of preparedness as well as to develop a program to enhance their security posture. States can also use this model to help prepare the communities within their state and can extend the concepts found within the model to state entities.

8. References

[1] IBM News, "Report finds online attacks shift toward profit", August 2, 2005, www.ibm.com/news/us/en/2005/08/2005_08_02.html

[2] Symantec Press Release, "Symantec Internet Security Threat Report Highlights Rise in Threats to Confidential Information", March 21, 2005, www.symantec.com/press/2005/n050321.html

[3] Waterman, Shaun, "Islamists Seek To Organize Hackers' Jihad in Cyberspace", August 26, 2005, *Washington Times*, P.9.

[4] Alexander, Keith, Welcoming Remarks, 10th Annual Colloquium for Information Systems Security Education, June 6, 2006, University of Maryland University College, Adelphi, MD.

[5] Paulk, Curtis, Chrissis, and Weber, "Capability Maturity Model℠ for Software, Version 1.l", Technical Report, CMU/SEI-93-TR-024, Carnegie Mellon University, February 1993.

[6] "System Security Engineering Capability Maturity Model® SSE-CMM® Model Description Document, Version 3.0", Carnegie Mellon University, June 15, 2003.

[7] "Government Emergency Telecommunications Service", National Communication Systems, http://gets.ncs.gov/.

[8] White, Gregory B. Glenn Dietrich, and Tim Goles, "Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events", *Proceedings of the 37th Hawaii International Conference on System Sciences*, 5-8 January 2004, Big Island, Hawaii.

[9] Conklin, Art and Gregory B. White, "e-Government and Cyber Security: The Role of Cyber Security Exercises", Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 4-7 January 2006, Kauai, Hawaii.